





功能规格书

如有任何变动，恕不预先通知

info@acs.com.hk
www.acs.com.hk

目录

图

1.0. 简介

本手册阐述了龙杰智能卡有限公司研发的 ACS 智能卡操作系统—版本 5.0（ACOS5）的特性与功能。

1.1. 特性

ACOS5 具有以下特性：

- 32K 字节 EEPROM 应用数据存储容量
- 符合 ISO 7816 第 1、2、3、4、8、9 部分
- 符合 ISO7816-2，具有 8 个触点
- 可转换的高速通讯波特率(9.6 Kbps 至 115.2 Kbps)
- 支持 ISO 7816 第 4 部分文件结构：透明、线性定长、线性变长、循环
- 支持 DES / 3DES / SHA1 / RSA 加密算法
- 可生成 RSA 密钥，高达 2048 位
- 支持 AES-128
- 符合 FIPS140-2 的随机数发生器
- 具有相互认证功能，能够生成会话密钥
- 具有安全报文发送功能，确保数据传输的保密性和真实性
- 多层次的安全访问等级
- 具有防拔插机制，确保文件头和系统信息受到保护
- 通用标准 EAL5+（芯片级）
- 符合 FIPS140-2 标准

1.2. 技术参数

1.2.1. 电气

- 工作电压 5V DC +/-10 %（Class A）、3V DC +/-10%（Class B）和 1.8V DC +/-10%（Class C）
- 最大电源电流：<20 mA
- ESD 保护：≤ 5 KV

1.2.2. EEPROM

- 容量：32K 字节
- EEPROM 使用寿命：50 万次擦写
- 数据保留时间：10 年

1.2.3. 环境温度

- 工作温度：-25 °C 至 85 °C
- 存储温度：-40 °C 至 100 °C

1.3. 符号和缩写

3DES	3 倍 DEA 算法 Triple DES
AES	高级加密标准 Advanced Encryption Standard
AMB	访问模式字节 Access Mode Byte
AMDO	访问模式数据对象 Access Mode Data Object
APDU	应用协议数据单元 Application Protocol Data Unit
AT	认证模板 Control Reference Template for Authentication
ATR	复位应答 Answer To Reset
CCT	密码校验和模板 Control Reference Template for Cryptographic checksum
CRT	中国余数定理(RSA)
CRT	控制引用模板 Control Reference Template
CT	保密模板 Control Reference Template for Confidentiality
DE	数据元素 Data Element
DES	数据加密标准 Data Encryption Standard
DF	专用/目录文件 Dedicated File
DO	数据对象 Data Object
DST	数字签名模板 Data Signature
EEPROM	电可擦除可编程只读存储器 Electrically Erasable Programmable Read-Only Memory
EF	基本文件 Elementary File
EF1	个人密码文件 PIN File
EF2	密钥文件 KEY File
ESD	静电释放 Electrostatic Discharge
HT	哈希模板 Control Reference Template for Hash-code
ISO	国际标准化组织 International Standard Organization
FCI	文件控制信息 File Control Information
FCP	文件控制参数 File Control Parameters
FDB	文件类型字节 File Descriptor Byte
LCSI	应用周期状态信息 Life Cycle Status Integer
LSb	最低有效位 Least Significant Bit
LSB	最低有效字节 Least Significant Byte
MAC	报文认证码 Message Authentication Code



MF	主控文件/目录 Master File
MRL	最大记录长度 Maximum Record Length
MSb	最高有效位 Most Significant Bit
MSB	最高有效字节 Most Significant Byte
MSE	管理安全环境 Managing Security Environment
NOR	记录的数量 Number Of Record
PSO	执行安全操作 Proceed Security Operation
RFU	保留为将来使用 Reserved for Future Use
RSA	由 Rivest、 Shamir 和 Adleman 三人共同发明的公钥加密算方法
SAC	标准安全属性 Security Attribute – Compact
SAE	扩展安全属性 Security Attribute – Expanded
SCB	安全条件字节 Security Condition Byte
SCDO	安全条件数据对象 Security Condition Data Object
SE	安全环境 Security Environment
SFI	短文件标识符 Short File Identifier
SHA	安全哈希算法 Security Hash Algorithm
SM	安全报文发送 Secure Messaging
SM-enc	带加密的安全报文(在本文档很多场合指的是加密+MAC) Secure Messaging with Encryption
SM-MAC	带 MAC 的安全报文 Secure Messaging with MAC
SM-Sign	用于确保真实性的安全报文 Secure Messaging with Sign
TLV	标签-长度-值 Tag-Length-Value
UQB	应用限定字节 Usage Qualifier Byte
XX_H	字节的十六进制位表示
||	连接 Concatenation
♁	按位异或 Bitwise Exclusive OR

info@acs.com.hk
www.acs.com.hk

2.0. 卡片管理

本节概述了卡层级的特性和管理功能。

2.1. 防拔插

ACOS5 采用防拔插机制保护卡片数据，避免由于卡片拔插导致的损坏（如在数据更新时突然从读写器中拔出卡片，或者读写器在卡片数据更新过程中发生机械故障）。卡片复位后，ACOS5 应用防拔插机制对相应区域进行必要的数据恢复。COS 将会把事先保存的数据返回至 EEPROM 原来的地址。

2.2. 卡应用状态

ACOS5 具有以下的状态：

1. 预个人化状态
2. 个人化状态
3. 用户状态

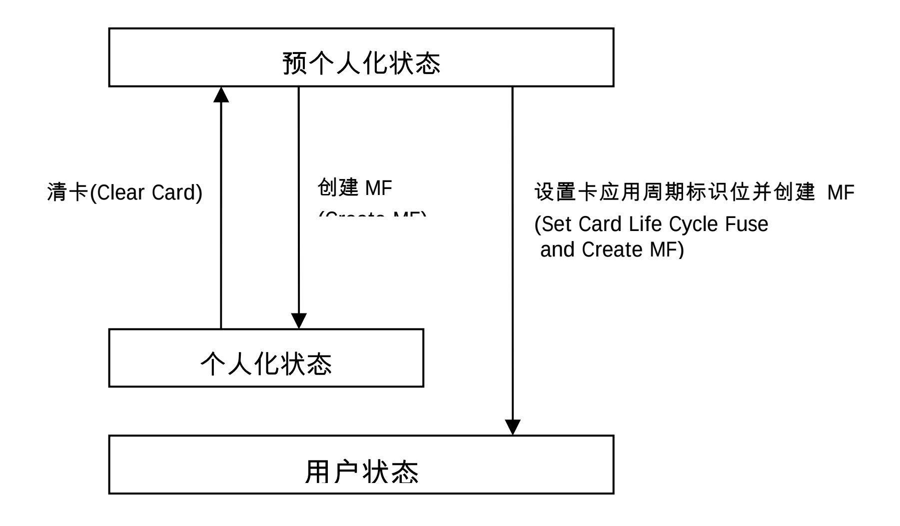


Figure 1. 卡片生命周期状态

预个人化状态 – 是卡的初始状态。卡没有文件系统。在此状态中，可以通过直接写卡的物理内存对 ATR TA1（通信速度）和历史字节进行个人化。用户可以根据规格说明书的属性创建主控文件。

个人化状态 – 一旦在前一阶段成功创建 MF 后，卡片即会进入本阶段。用户不再能够直接访问卡片头块。就像在操作模式中一样，用户能够创建和测试 MF 下的文件。

调用清卡 CLEAR CARD 命令将会使卡返回至预个人化状态。极力推荐使用 ACOS5 SDK 的清卡工具。它不仅可以清卡，而且可以将关键的工厂更新加载至卡内。

如果应用程序开发员希望只有在验证后才允许清卡，则可以在 MF 和 DF 层级设置 SAE 条件，规

定只有在 PIN 认证或密钥验证后才能够执行清卡命令。

用户状态 – 相当于卡片的操作模式。所有的卡片设置（例如安全性、文件组织等等）都是在此状态中生效。

2.3. 复位应答 (ATR)

硬件复位后（如上电），卡片按照 ISO 7816 第 3 部分规定传送复位应答（ATR），格式与 ACOS2/3 相同。ACOS5 支持正向约定的 T=0 协议。以下是默认的 ATR，关于 ATR 选项的详细描述请参看 ISO 7816 第 3 部分。

2.3.1. 自定义ATR

ACOS5 的 ATR 可以自定义，包括修改卡片速度或者在历史字符串中写入具体的身份信息。新的 ATR 必须符合 ISO7816 第 3 部分，否则卡片可能在下次上电或者复位时可能变得没有反应或者不可恢复之前状态。

ATR 可以在卡片的预个人化阶段自定义。

3.0. 文件系统

3.1. 多层次的文件系统

ACOS5 的文件系统和结构完全符合的文件系统和结构完全符合 ISO 7816 第 4 部分的规定。该文件系统非常类似于现代计算机操作系统。该文件的根是主文件（MF）。卡中的每个应用或数据文件组均可包含在称为专用文件（DF）的目录中。每个 DF 或 MF 都可以在目录下的基本文件（EF）中存储数据

ACOS10 允许任意深度的 DF 树结构。也就是说，DF 可以嵌套，如下图所示。

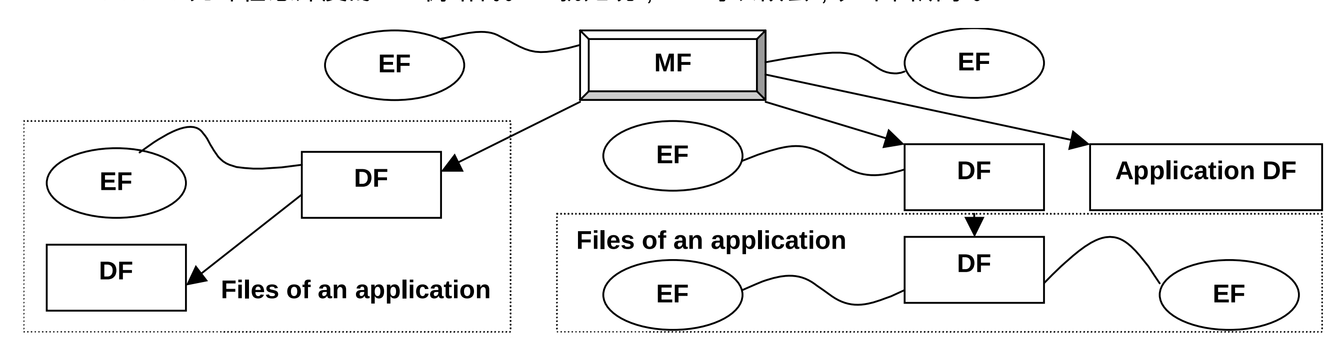


Figure 2. 多层次的 DF 文件系统

3.2. 文件头数据结构

ACOS5 通过文件组织用户 EEPROM 区。每个文件都有一个文件头，即一个描述文件属性的数据块。文件头模块的知识将有助于应用程序开发人员准确地规划 EEPROM 空间的使用。文件头块包括以下域：

文件头中的每一项将在后面的章节中描述。

3.3. 内部安全文件

COS 的运作取决于与安全相关的内部文件的内容。通常，一个 DF 应该具有：

（1）一个密钥文件，用于储存用于校验的 PIN 码（称为 EF1）；

（2）一个密钥文件，用于储存用于验证的密钥代码（称为 EF2）；

（3）一个 SE 文件，用于储存安全条件和模板；

（4）一个非对称的密钥 EF 文件，用于储存 RSA 密钥。

密钥文件时一种内部线性可变文件。它可能包含（1）PIN 数据结构或者（2）密钥数据结构。

4.0. 安全机制

文件命令受制于目标文件（或当前的 DF）的安全访问条件。这些条件是基于由系统当前维护的个人密码和密钥。如果对应的 PIN 或 KEY 的校验或认证通过，卡的命令将被允许。

全局 PIN 直接存储在 MF 的 PIN 文件(EF1)，局部 PIN 存储在当前选择的 DF 的 PIN 文件。同样，全局 KEY 直接存储在 MF 的 KEY 文件(EF2)，局部 KEY 存储在当前选择的 DF 的 KEY 文件。最多允许同时存在 31 个全局 PIN,31 个局部 PIN,31 个全局 KEY,31 个局部 KEY.

4.1. 文件安全属性

每个文件(MF、DF 或 EF)的文件头模块中都设置有一套安全属性。安全属性设置模式分为两种：标准安全属性（SAC）和扩展安全属性（SAE）。

4.2. 安全环境 (SE)

安全条件在 SE 文件中存储与编码。每个 DF 都有一个指定的 SE 文件（建立 DF 文件的时候指定），该文件的文件标识符(FID)存储在该 DF 的文件头模块中，SE 记录格式如下：

<SE ID Template> <SE DO Template>

4.3. 认证

相互认证是卡片与读卡设备之间相互认证对方真实性与合法性的过程。相互认证成功执行以后会产生一个会话密钥（*Session Key*），该会话密钥只在会话中才有效。这个会话我们这样定义：在相互认证成功执行以后，直到卡片的重新复位或者另外一次相互认证的执行。执行 SELECT FILE（选择文件）命令也可以结束一个会话。

4.4. 安全报文

安全报文发送功能（SM）确保 ACOS5 和终端/服务器之间通信的安全性。ACOS5 支持安全报文发送，用于验证和确保机密性。

安全报文模式分为两种，可分别用于两种不同的情况。第一种模式是用于确保真实性的报文(SM-sign)，另一种是用于确保保密性的报文(SM-EMC)。这两种模式均可应用于命令和回应数据。

5.0. 生命支持应用

这些产品的设计并非用于生命支持设备或系统，在这些设备或系统中对这些产品的误操作可能导致人身伤害。如果 ACS 客户将这些产品使用于或者销售用于此类应用，则他们应该自行承担相应的风险，而且同意赔偿由于不当使用或销售从而给 ACS 造成的损失。



6.0. 联系信息

如需了解其他信息，请访问ACS网站http://www.acs.com.hk。

如需销售咨询，请发送邮件至info@acs.com.hk。